

# The maximum output $p$ -norm of quantum channels is not multiplicative for any $p > 2$

Andreas Winter<sup>1,2</sup>

<sup>1</sup>*Department of Mathematics, University of Bristol, Bristol BS8 1TW, U.K.*

<sup>2</sup>*Quantum Information Technology Lab, National University of Singapore, 2 Science Drive 3, Singapore 117542\**

(Dated: 30 July 2007)

**Introduction and context.** In quantum information theory, just as in its classical counterpart, operational capacities (of information transmission over channels, of state distillation or preparation procedures, and the like) are most naturally expressed in terms of (von Neumann) entropies  $S(\rho) = -\text{Tr } \rho \log \rho$  [6]. Usually the formulas involve optimisation of the entropic quantity in question over finitely many parameters; examples include the *entanglement of formation* of a bipartite state [5], the so-called *Holevo capacity* of a quantum channel [9], or the *minimum output entropy* of a channel [3].

Since we are dealing with an asymptotic theory of information – in the simplest case, this means looking at many independent realisations of the state or channel under considerations – the natural and imminently important question arises, if these quantities are extensive; in information theory, this is the additivity problem, which asks if quantities like entanglement of formation, Holevo capacity, minimum output entropy, etc. are additive under tensor products. While all these conjectures remain open to date, interestingly, Shor [15] has shown that the three mentioned are actually equivalent. See [10] for a general exposition, and pointers to the literature. Here, we will deal with a related conjecture, on minimum output Rényi entropies, and exhibit counterexamples for all Rényi parameters  $p > 2$ .

**The conjecture.** For quantum channels  $\mathcal{N}$  (i.e., completely positive, trace preserving [cptp] maps between – finite – quantum systems) one considers the maximum output  $p$ -norm ( $p > 1$ ),

$$\nu_p(\mathcal{N}) = \max_{\rho} \|\mathcal{N}(\rho)\|_p, \quad (1)$$

where the maximum is over all normalised positive semidefinite density operators, and  $\|X\|_p = (\text{Tr } |X|^p)^{1/p}$  is the operator  $p$ -norm. W.l.o.g. the maximisation may be restricted to pure states  $\rho = |\psi\rangle\langle\psi|$ . In conjunction with the conjectured additivity of the minimum output entropy of the channel, it has been conjectured that  $\nu_p$  is *multiplicative* for  $p > 1$  [3]:

$$\nu_p(\mathcal{N}_1 \otimes \mathcal{N}_2) = \nu_p(\mathcal{N}_1) \nu_p(\mathcal{N}_2). \quad (2)$$

Indeed, this multiplicativity for  $p$  sufficiently close to 1 would imply the additivity of the minimum output entropy of the channel, and hence [15] the other “standard” additivity conjectures of quantum information theory. An easy way of making this link is to consider Rényi  $p$ -entropy,  $S_p(\rho) = \frac{1}{1-p} \log \text{Tr } \rho^p$ , instead of the  $p$ -purity  $\text{Tr } \rho^p$ . Clearly then, the minimum output  $p$ -entropy of the channel is  $\frac{p}{1-p} \log \nu_p(\mathcal{N})$ , turning multiplicativity into additivity. To finish the argument, all that is needed is the observation that  $\lim_{p \rightarrow 1} S_p(\rho) = S(\rho)$ .

From the elementary multiplicativity of the  $p$ -norm itself, the inequality “ $\geq$ ” in (2) is trivial, so the question is always if “ $\leq$ ” holds. Now, Holevo and Werner [11] have shown that (2) cannot

---

\*Electronic address: a.j.winter@bris.ac.uk

hold universally: there is a channel  $\mathcal{N}_{\text{HW}}$  which provides a counterexample for  $p > 4.79$ , in the sense that for all such  $p$ ,

$$\nu_p(\mathcal{N}_{\text{HW}} \otimes \mathcal{N}_{\text{HW}}) > \nu_p(\mathcal{N}_{\text{HW}})^2.$$

On the other hand, King and Ruskai have argued [14] that (2) should still hold true for  $1 < p \leq 2$ . Incidentally, for the Holevo-Werner channel  $\mathcal{N}_{\text{HW}}$ , and a whole class containing it, multiplicativity has indeed been shown for  $1 < p \leq 2$  and arbitrary number of tensor factors [1]. This poses the natural problem of constructing counterexamples to (2) for all  $p > 2$ . In the rest of the paper, we show that approximately randomising channels [8] provide exactly that.

**Random unitary channels.** These are channels of the form

$$\mathcal{N} : \rho \mapsto \frac{1}{n} \sum_{i=1}^n V_i \rho V_i^\dagger, \quad (3)$$

with unitaries  $V_i$  of the underlying  $d$ -dimensional Hilbert space (More generally, one could allow variable probability weights for different  $V_i$ , but we won't need that here.)

Following [8], we call  $\mathcal{N}$   $\epsilon$ -randomising, if

$$\forall \rho \quad \left\| \mathcal{N}(\rho) - \frac{1}{d} \mathbb{1} \right\|_\infty \leq \frac{\epsilon}{d}. \quad (4)$$

There, it is shown that for  $0 < \epsilon < 1$ ,  $\epsilon$ -randomising channels exist in all dimensions  $d > \frac{10}{\epsilon}$ , with  $n = \frac{134}{\epsilon^2} d \log d$  – in fact, randomly picking the  $V_i$  from the Haar measure on the unitary group will, with high probability, yield such a channel.

**Lemma 1.** For a random unitary channel  $\mathcal{N}$  and its complex conjugate,  $\overline{\mathcal{N}} : \rho \mapsto \frac{1}{n} \sum \overline{V_i} \rho \overline{V_i}^\dagger$ , one has  $\nu_p(\mathcal{N} \otimes \overline{\mathcal{N}}) \geq \frac{1}{n}$ .

*Proof.* We use the maximally entangled state  $\Phi_d = \frac{1}{d} \sum_{\alpha\beta} |\alpha\alpha\rangle\langle\beta\beta|$  as test state:

$$\begin{aligned} \nu_p(\mathcal{N} \otimes \overline{\mathcal{N}}) &\geq \|(\mathcal{N} \otimes \overline{\mathcal{N}})\Phi_d\|_p \\ &= \left\| \frac{1}{n^2} \sum_{ij=1}^n (V_i \otimes \overline{V_j}) \Phi_d (V_i \otimes \overline{V_j})^\dagger \right\|_p \\ &= \left\| \frac{1}{n} \Phi_d + \frac{1}{n^2} \sum_{i \neq j} (V_i \otimes \overline{V_j}) \Phi_d (V_i \otimes \overline{V_j})^\dagger \right\|_p \geq \frac{1}{n}, \end{aligned}$$

where in the third line we have invoked the  $U \otimes \overline{U}$ -invariance of  $\Phi_d$ , for all  $n$  occurrences of  $i = j$ . For the final inequality, observe that the largest eigenvalue  $\lambda_1$  of  $\omega := (\mathcal{N} \otimes \overline{\mathcal{N}})\Phi_d$  is  $\geq \frac{1}{n}$ , and denoting the other eigenvalues  $\lambda_\alpha$ ,  $\|\omega\|_p = (\sum_\alpha \lambda_\alpha^p)^{1/p} \geq \lambda_1$ , and we are done.  $\square$

**Lemma 2.** If the channel  $\mathcal{N}$  is  $\epsilon$ -randomising, then, with  $p > 1$ ,

$$\nu_p(\mathcal{N}) = \nu_p(\overline{\mathcal{N}}) \leq \left( \frac{1+\epsilon}{d} \right)^{1-1/p}.$$

*Proof.* Clearly,  $\mathcal{N}$  and  $\overline{\mathcal{N}}$  have the same maximum output  $p$ -norm. For the former, observe that the  $\epsilon$ -randomising condition implies, for arbitrary input state  $\rho$ ,  $\|\mathcal{N}(\rho)\|_\infty \leq \frac{1+\epsilon}{d}$ , in other words, all eigenvalues  $\lambda_\alpha$  of the output state  $\mathcal{N}(\rho)$  are bounded between 0 and  $\frac{1+\epsilon}{d}$ , besides summing to 1.

Hence, by convexity of the function  $x \mapsto x^p$ , the  $p$ -norm  $\|\mathcal{N}(\rho)\|_p = (\sum_\alpha \lambda_\alpha^p)^{1/p}$  is maximised, under these constraints, at a spectrum with largest eigenvalue  $\frac{1+\epsilon}{d}$ , with multiplicity  $\frac{d}{1+\epsilon}$ , and the remaining eigenvalues 0, yielding  $\|\mathcal{N}(\rho)\|_p = (\sum_\alpha \lambda_\alpha^p)^{1/p} \leq \left(\frac{d}{1+\epsilon} \left(\frac{1+\epsilon}{d}\right)^p\right)^{1/p} = \left(\frac{1+\epsilon}{d}\right)^{1-1/p}$ .  $\square$

**Main result.** Now fix any  $0 < \epsilon < 1$ , and a family of  $\epsilon$ -randomising maps  $\mathcal{N}$  for all sufficiently large dimensions  $d$  and  $n = O(d \log d)$  as above. Then, for any  $p > 2$  and sufficiently large  $d$ ,

$$\nu_p(\mathcal{N})\nu_p(\overline{\mathcal{N}}) \leq \left(\frac{1+\epsilon}{d}\right)^{2-2/p} \ll \frac{1}{n} \leq \nu_p(\mathcal{N} \otimes \overline{\mathcal{N}}), \quad (5)$$

by Lemmas 1 and 2, and since  $2 - 2/p > 1$ . I.e., for this family of channels, the maximum output  $p$ -norm is strictly supermultiplicative, eventually.  $\square$

**Discussion.** The counterexamples to the multiplicativity of the output  $p$ -norm for  $p > 2$  provided here are interesting in that they are random unitary channels, which are among the simplest truly quantum maps – in fact, the first proofs of multiplicativity for unital qubit channels [12] and depolarising channels [13] relied on this kind of channel structure. Indeed, unital qubit channels are always random unitary channels (that is our case with  $d = 2$ ), and King [12] shows multiplicativity for such channels at all  $p > 1$  – there is no conflict with our result here, as the bound on  $n$  becomes better than  $d^2$  only for rather large dimension  $d$ .

We observe, furthermore, that  $p = 2$  is indeed the limit of validity of the counterexample(s), since  $n \geq d$  for any  $\epsilon$ -randomising map.

Note, however, that in the condition of  $\epsilon$ -randomisation, it is not so crucial to have  $\epsilon$  small: looking at the above argument, we see that indeed any constant, or even any mildly (say, poly-logarithmically), in  $d$ , growing  $\epsilon$  will do. Still, it seems that we have to rely on the strong randomisation via Haar measure unitaries from [8]: all other, more or less explicit, constructions (by Ambainis and Smith [2] or via iterated quantum expander maps [4, 7]) only give us bounds in the 2-norm, which do imply bounds on the output  $p$ -norm but they are too weak for the present purpose. As a consequence, we don't have any *explicit* counterexamples, but really only a proof of their existence – it remains as an open problem to “derandomise” our argument.

**Note added.** Since the posting of this work on the arXiv, Patrick Hayden (arXiv:0707.3291) has shown how to extend the range of the counterexamples to all  $p > 1$ . Interestingly, as  $p$  gets closer to 1, the dimension of the output has to grow to infinity for a violation to occur, so the original additivity conjecture (at  $p = 1$ ) is still left intact. This dramatic finding now focusses the attention on the question of the multiplicativity of the *minimum* output  $p$ -norm for  $0 \leq p \leq 1$ .

**Acknowledgments.** The author is supported by the U.K. EPSRC (“QIP IRC” and an Advanced Research Fellowship) and the EU project “QAP”. Thanks to Patrick Hayden, Debbie Leung and Beth Ruskai for discussions on the multiplicativity conjecture and possible counterexamples, starting at the BIRS workshop “Operator Structures in Quantum Information”, February 2007, and to Toby Cubitt and Ashley Montanaro for conversations about multiplicativity at  $p = 0$ .

- 
- [1] R. Alicki, M. Fannes, “Note on Multiple Additivity of Minimal Renyi Entropy Output of the Werner-Holevo Channels”, *Open Systems Inf. Dyn* **11**(4):339-342 (2004); arXiv:quant-ph/0407033.
  - [2] A. Ambainis, A. Smith, “Small pseudo-random families of matrices: Derandomizing approximate quantum encryption”, in: *Proc. RANDOM*, Springer LNCS 3122, pp. 249-260 (2004); arXiv:quant-ph/0404075.

- [3] G. G. Amosov, A. S. Holevo, R. F. Werner, "On some additivity problems in quantum information theory", arXiv:math-ph/0003002 (2000).
- [4] A. Ben-Aroya, A. Ta-Shma, "Quantum expanders and the quantum entropy difference problem", arXiv:quant-ph/0702129 (2007).
- [5] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wootters, "Mixed-state entanglement and quantum error correction", Phys. Rev. A **54**(5):3824-3851 (1996).
- [6] C. H. Bennett, P. W. Shor, "Quantum Channel Capacities", Science **303**:1784-1786 (2004).
- [7] M. B. Hastings, "Random Unitaries Give Quantum Expanders", arXiv[quant-ph]:0706.0556 (2007).
- [8] P. Hayden, D. Leung, P. W. Shor, A. Winter, "Randomizing Quantum States: Constructions and Applications", Comm. Math. Phys. **250**(2):371-391 (2004); arXiv:quant-ph/0307104.
- [9] A. S. Holevo, "The capacity of the quantum channel with general signal states", IEEE Trans. Inf. Theory **44**(1):269-273 (1998); arXiv:quant-ph/9611023. B. Schumacher, M. D. Westmoreland, "Sending classical information via noisy quantum channels", Phys. Rev. A **56**(1):131-138 (1997).
- [10] A. S. Holevo, "Additivity of classical capacity and related problems", <http://www.imaph.tu-bs.de/qi/problems/10.html>.
- [11] A. S. Holevo, R. F. Werner, "Counterexample to an additivity conjecture for output purity of quantum channels", J. Math. Phys. **43**(9):4353-4357 (2002); arXiv:quant-ph/0203003.
- [12] C. King, "Additivity for unital qubit channels", J. Math. Phys. **43**:4641-4653 (2002); arXiv:quant-ph/0103156.
- [13] C. King, "The capacity of the quantum depolarizing channel", IEEE Trans. Inf. Theory **49**:221-229 (2003); arXiv:quant-ph/0204172.
- [14] C. King, M.-B. Ruskai, "Comments on multiplicativity of maximal p-norms when  $p=2$ ", Quant. Inf. Comput. **4**(6&7):500-512 (2004); arXiv:quant-ph/0401026.
- [15] P. W. Shor, "Equivalence of Additivity Questions in Quantum Information Theory", Comm. Math. Phys. **246**(3):453-472 (2004); arXiv:quant-ph/0305035.